

# Cryptographic quantum bound on nonlocality

Satoshi Ishizaka

*Graduate School of Integrated Arts and Sciences, Hiroshima University,  
1-7-1 Kagamiyama, Higashi-Hiroshima, 739-8521, Japan*

(Dated: February 6, 2017)

Information causality states that the information obtainable by a receiver cannot be greater than the communication bits from a sender, even if they utilize no-signaling resources. This physical principle successfully explains some boundaries between quantum and postquantum nonlocal correlations, where the obtainable information reaches the maximum limit. We show that no-signaling resources of pure partially entangled states produce randomness (or noise) in the communication bits, and achievement of the maximum limit is impossible, i.e., the information causality principle is insufficient for the full identification of the quantum boundaries already for bipartite settings. The nonlocality inequalities such as so-called the Tsirelson inequality are extended to show how such randomness affects the strength of nonlocal correlations. As a result, a relation followed by most of quantum correlations in the simplest Bell scenario is revealed. The extended inequalities reflect the cryptographic principle such that a completely scrambled message cannot carry information.

## I. INTRODUCTION

It was shown by Bell that the nonlocal correlations predicted by quantum mechanics are inconsistent with local realism [1]. The nonlocal correlations do not contradict the no-signaling principle that prohibits instantaneous communication. However, it was found that the set of quantum correlations is strictly smaller than the set of no-signaling correlations [2, 3]. Concretely, a particular type of the Bell inequality, the Clauser-Horne-Shimony-Holt (CHSH) inequality [4], was shown to be violated up to 4 in general no-signaling correlations [3], while from the Tsirelson inequality [2] the violation is bounded by  $2\sqrt{2}$  in quantum correlations. Since then, many efforts have been made to search for a simple physical principle to close this discrepancy. See [5–7] for a good review.

Information causality (IC) [8] is such a physical principle. Consider two remote parties, Alice and Bob, who share no-signaling nonlocal resources such as entangled states. When Alice sends a message to Bob, IC states that the total information obtainable by Bob cannot be greater than the number of the message bits even if they utilize the no-signaling resources [8]. A powerful necessary condition for respecting the IC principle was derived by considering an explicit communication protocol [8]. The condition, called the IC inequality hereafter, successfully explains the Tsirelson inequality, and even explains some curved boundaries between quantum and postquantum correlations [8, 9]. At those quantum boundaries, the protocol achieves the maximum limit of the obtainable information (the number of the message bits). It is then expected that, for every quantum boundary, there exists a protocol for which the maximum limit is achieved.

Apart from searching for physical principles, the identification of the quantum boundaries is originally a difficult problem. Indeed, the analytical necessary and sufficient criterion for the identification has not been given yet even in the simplest Bell scenario, although the Tsirelson-Landau-Masanes (TLM) criterion [10–12] is known for a

case of unbiased marginal probabilities (explain later).

In this paper, we show that pure partially entangled states, which were shown to give rise to boundary correlations [13–16], produce randomness in the message, and achievement of the maximum limit is impossible no matter what protocol is executed. Hence, the IC principle is insufficient for the full identification of the quantum boundaries already for bipartite settings (similar results have been obtained in multipartite settings [17, 18]). We extend the nonlocality inequalities to include the effects of the randomness. As a result, a relation followed by most of quantum correlations, including both cases of unbiased and biased marginals, is revealed. Moreover, we show that the derived inequalities reflect the cryptographic principle such that a completely scrambled message cannot carry information [19]. The inequalities reflecting the cryptographic principle contain a quantity defined in quantum mechanics, and the principle cannot immediately exclude postquantum correlations by itself, but tells us a way to determine the quantum boundaries. Note that a similar principle for a different type of randomness was considered in [20].

Let us here show a simple example to clarify what we mean by randomness. Consider the simplest Bell scenario, where Alice is given a random bit  $x$  and performs the measurement on the partially entangled state  $\sqrt{2/3}|00\rangle + \sqrt{1/3}|11\rangle$  in the basis  $|0\rangle/|1\rangle$  for  $x = 0$  or  $(|0\rangle \pm |1\rangle)/\sqrt{2}$  for  $x = 1$ , and obtains the outcome  $a$ . Suppose that Bob somehow knows that  $x$  was 1. However, he still cannot determine the value of  $a$  completely, because his local state is  $\sqrt{2/3}|0\rangle + \sqrt{1/3}|1\rangle$  for  $a = 0$  or  $\sqrt{2/3}|0\rangle - \sqrt{1/3}|1\rangle$  for  $a = 1$ , which are nonorthogonal. This means that  $a$  has some uncertainty indeterminate for Bob, and the uncertainty acts as randomness (or noise) if  $a$  is used for the transmission of the information of  $x$  (the details are discussed in Sec. IV). As a result, the obtainable information of Bob is reduced. This affects the quantum bound of the CHSH inequality, and the violation is reduced to  $2\sqrt{17/9}$  [see Eq. (2) below] from the maximum value of  $2\sqrt{2}$ .

This paper is organized as follows. In Sec. II, we extend the Tsirelson inequality, the IC inequality, and the Landau inequality (of the TLM criterion) by including the state-dependent quantity measuring the orthogonality between Bob's local states, because nonorthogonality is key to the randomness as in the above example. In Sec. III, we discuss the tightness of the derived Landau-type inequality, and show that the inequality is widely saturated for both boundary and non-boundary correlations even in the case of biased marginals. We then discuss the information theoretical aspects of the derived IC-type inequality in Sec. IV, where the connection to the cryptographic principle and the insufficiency of the IC principle are shown. In Sec. V, we show an example of how to determine the quantum boundaries under the cryptographic principle. A summary is given in Sec. VI.

## II. BOUNDS ON NONLOCALITY

To begin with, let us derive the inequalities discussed in this paper. The derivation is surprisingly simple. Consider the simplest Bell scenario, where Alice and Bob share a quantum state, Alice (Bob) performs a measurement depending on a given bit  $x$  ( $y$ ) to obtain the outcome bit  $a$  ( $b$ ). Their shared state is a pure or mixed state denoted by  $\rho$ . We use the shorthand notation  $\langle \dots \rangle$  for  $\text{tr} \rho \dots$ . Without loss of generality, we can assume that they perform projective measurements, because no assumption is made about the system dimension. The observable of Alice (Bob), denoted by  $A_x$  ( $B_y$ ), then satisfies  $A_x^2 = B_y^2 = I$  with  $I$  being the identity operator. The projector of the measurement for Alice's outcome  $a$  is given by  $P_{a|x} = (I + (-1)^a A_x)/2$ , and for Bob's outcome  $b$  by  $Q_{b|y} = (I + (-1)^b B_y)/2$ . Let us then consider the weighted CHSH expression [21] of the form:

$$\mathcal{B} = \sum_y t_y s_x (-1)^{xy} \langle A_x \otimes B_y \rangle = \sum_y t_y E_y, \quad (1)$$

where  $t_y$  and  $s_x$  are real non-negative parameters, and  $E_y \equiv s_0 \langle A_0 \otimes B_y \rangle + s_1 (-1)^y \langle A_1 \otimes B_y \rangle$  is introduced for later convenience. If we define  $X_x \equiv t_0 B_0 + (-1)^x t_1 B_1$ , it can be seen that  $X_0^2 + X_1^2 = 2(t_0^2 + t_1^2)I$ , and we obtain the Tsirelson-type inequality as follows:

$$\begin{aligned} \mathcal{B} &= \sum_x s_x \sqrt{\langle I \otimes X_x^2 \rangle} \frac{\langle A_x \otimes X_x \rangle}{\sqrt{\langle I \otimes X_x^2 \rangle}} \leq \sum_x s_x \sqrt{\langle I \otimes X_x^2 \rangle} \tilde{D}_x \\ &\leq \sqrt{2(t_0^2 + t_1^2)(s_0^2 \tilde{D}_0^2 + s_1^2 \tilde{D}_1^2)}, \end{aligned} \quad (2)$$

where we used  $\sum_x \langle I \otimes X_x^2 \rangle = 2(t_0^2 + t_1^2)$  as a constraint in the last inequality. The quantity  $\tilde{D}_x$  is defined by

$$\tilde{D}_x \equiv \max_X \frac{\langle A_x \otimes X \rangle}{\sqrt{\langle I \otimes X^2 \rangle}} = \max_X \frac{\text{tr} X(\rho_{0|x} - \rho_{1|x})}{\sqrt{\text{tr} X^2(\rho_{0|x} + \rho_{1|x})}}, \quad (3)$$

where the maximization is taken over all Hermitian operators  $X$ , and  $\rho_{a|x} = \text{tr}_A(P_{a|x} \otimes I)\rho$  is Bob's subnormalized state when Alice is given  $x$  and her outcome is  $a$ .

The quantity  $\tilde{D}_x$  is quite analogous to the generalized trace distance  $\bar{D}_x = \text{tr}|\rho_{0|x} - \rho_{1|x}|$  (the extension of the trace distance to subnormalized states). Indeed, both agree with each other for the case of pure states. For the other general cases,  $\tilde{D}_x \geq \bar{D}_x$ . See Appendix A for the proofs of those properties. It is obvious from the definition of Eq. (3) that  $\tilde{D}_x \leq 1$ , because it is the inner product of the two normalized states  $(A_x \otimes I)|\psi\rangle$  and  $(I \otimes X)|\psi\rangle / \sqrt{\langle \psi | I \otimes X^2 | \psi \rangle}$  (consider a purification  $|\psi\rangle$  if  $\rho$  is a mixed state), and the inner product is ensured to be real [10, 22]. Note that a different type of quantum bounds using the trace distance was shown in [23]. Since the envelope of the boundaries of Eq. (2) in the  $(E_0, E_1)$ -space is a quarter-circle, considering the symmetry with respect to  $B_y \rightarrow -B_y$  and putting  $s_0 = s_1 = 1/2$ , we have the IC-type inequality:

$$E_0^2 + E_1^2 \leq \frac{\tilde{D}_0^2 + \tilde{D}_1^2}{2}. \quad (4)$$

Note that  $E_0$  and  $E_1$  coincides with  $E_I$  and  $E_{II}$  in [8], respectively.

In the same technique as above, a tighter quantum bound is obtained by considering more general weight parameters as follows:

$$\sum_{xy} s_x u_{xy} (-1)^{xy} \langle A_x \otimes B_y \rangle \leq \left[ \sum_{xy} u_{xy}^2 \right]^{\frac{1}{2}} \left[ \sum_x s_x^2 \tilde{D}_x^2 \right]^{\frac{1}{2}}, \quad (5)$$

where  $s_x$  and  $u_{xy}$  are real parameters satisfying  $u_{00}u_{01} = u_{10}u_{11}$ . When  $\tilde{D}_0, \tilde{D}_1 > 0$ , the necessary and sufficient condition for the above inequality is given by

$$\begin{aligned} \left| \tilde{C}_{00}\tilde{C}_{01} - \tilde{C}_{10}\tilde{C}_{11} \right| &\leq (1 - \tilde{C}_{00}^2)^{\frac{1}{2}}(1 - \tilde{C}_{01}^2)^{\frac{1}{2}} \\ &\quad + (1 - \tilde{C}_{10}^2)^{\frac{1}{2}}(1 - \tilde{C}_{11}^2)^{\frac{1}{2}}, \end{aligned} \quad (6)$$

where  $\tilde{C}_{xy} \equiv \langle A_x \otimes B_y \rangle / \tilde{D}_x \equiv C_{xy} / \tilde{D}_x$ . The derivation is given in Appendix B. This is an extension of the Landau inequality [11]. The Landau inequality is a representation of the TLM criterion, and hence is necessary and sufficient so that a given set of the conditional probabilities  $\{p(ab|xy)\}$  (or a given set of  $\{C_{xy}\}$ ) is quantum realizable in the case of unbiased marginals such that  $p(a|x) = p(b|y) = 1/2$ . It is known that the Navascués-Pironio-Acín (NPA) inequality [24, 25] gives a tighter bound than the Landau inequality for the case of biased marginals. It is also possible to extend the NPA inequality to include  $\tilde{D}_x$  as shown in Appendix B.

The above inequalities all represent the effects of the nonorthogonality between Bob's local states for  $a=0$  and  $1$ . Indeed, when  $\rho_{0|x}$  and  $\rho_{1|x}$  are orthogonal for both  $x=0$  and  $1$ , we have  $\tilde{D}_0 = \tilde{D}_1 = 1$ , and those reproduce the inequalities known so far. Note that  $\tilde{D}_x = 1$  if and only if  $\tilde{D}_x = 1$  (see Appendix A) and so also in the case of  $\text{tr} \rho_{0|x} = 0$  or  $\text{tr} \rho_{1|x} = 0$ . This is included in the orthogonal case throughout this paper.

### III. TIGHTNESS OF BOUNDS

The inequalities derived in Sec. II must hold for all physical realizations (by projective measurements). A nonlocal correlation is generally identified by the set of conditional probabilities  $\{p(ab|xy)\}$ , and the left-hand side of e.g., Eq. (5) is determined by  $\{p(ab|xy)\}$  only (for a fixed weight). On the other hand, the right-hand side is monotonically increasing with respect to  $\tilde{D}_x$ . It is then found that, if a set  $\{p(ab|xy)\}$  saturates the Landau inequality [i.e., the equality of Eq. (5) holds with  $\tilde{D}_0 = \tilde{D}_1 = 1$  by appropriately chosen weight parameters], the realization that produces the same  $\{p(ab|xy)\}$  but with  $\tilde{D}_x < 1$  is not allowed. Namely, we have the following:

**Lemma 1.** *For every correlation that saturates the Landau inequality, there is no realization such that Bob's subnormalized states  $\rho_{0|x}$  and  $\rho_{1|x}$  are nonorthogonal. The same holds for Alice's states.*

Note that this is the case of the NPA inequality by Eq. (B2). Note further that Lemma 1 is consistent with the fact that the nonclassical boundary correlations with unbiased marginals are all used for the self-testing of the maximally entangled state of two qubits, i.e., solely realized by the maximally entangled state [26], because every boundary correlation with unbiased marginals is given by the saturation of the Landau inequality.

In the case of the Landau-type inequality Eq. (6) that includes  $\tilde{D}_x$ , the saturation does not necessarily imply that the correlation is located at a boundary. Rather, the inequality is widely saturated even for non-boundary correlations. To see this, let us consider the completely random correlation  $\mathbf{I}$  given by  $p(ab|xy) = 1/4$  ( $\forall a, b, x, y$ ), which is realized by the maximally mixed state of two qubits  $\rho_{AB} = \frac{1}{4}I_A \otimes I_B$ , where  $C_{xy} = 0$  and  $\tilde{D}_x = 0$ . Then, if Eq. (6) is saturated for a correlation  $\mathbf{p}$  by some realization, it is also done for  $\mathbf{q}$  of the form

$$\mathbf{q} = \lambda \mathbf{p} + (1 - \lambda) \mathbf{I}, \quad (7)$$

where  $0 \leq \lambda \leq 1$ . This is because, when  $\mathbf{p}$  is realized by  $\rho_{AB}^{\mathbf{p}}$ ,  $\mathbf{q}$  is realized by the shared state of

$$\rho_{AB}^{\mathbf{p}} \otimes (\frac{1}{4}I_A \otimes I_B) \otimes [\lambda|00\rangle\langle 00| + (1 - \lambda)|11\rangle\langle 11|]_{AB} \quad (8)$$

such that Alice and Bob switch their measured states (and the corresponding measurements) between  $\rho_{AB}^{\mathbf{p}}$  and  $\frac{1}{4}(I_A \otimes I_B)$  according to the shared randomness produced by  $\lambda|00\rangle\langle 00| + (1 - \lambda)|11\rangle\langle 11|$ , and it is found from the closed form of  $\tilde{D}_x$  (see Appendix A) that  $\tilde{D}_x$  for  $\mathbf{q}$  and  $\mathbf{p}$  are related through  $\tilde{D}_x^{\mathbf{q}} = \lambda \tilde{D}_x^{\mathbf{p}} + (1 - \lambda) \tilde{D}_x^{\mathbf{I}} = \lambda \tilde{D}_x^{\mathbf{p}}$ , and hence  $\tilde{C}_{xy}^{\mathbf{q}} = \tilde{C}_{xy}^{\mathbf{p}}$  holds. This implies that, if Eq. (6) is saturated for every boundary of the set of quantum correlations, the inequality is saturated for all correlations inside the set. This is indeed the case of unbiased marginals, because the inequality is saturated for every boundary with  $\tilde{D}_0 = \tilde{D}_1 = 1$ , and we obtain the following:

**Lemma 2.** *For every correlation with unbiased marginals, there always exists a realization such that the equality holds in Eq. (6).*

An important observation is that the inequality is saturated even for the case of biased marginals. A two-qubit realization to give the maximal violation of the Bell expression  $\beta\langle A_0 \rangle + \alpha\langle A_0 B_0 \rangle + \alpha\langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$  was shown in [14], where the partially entangled state  $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$  produces the boundary correlations with biased marginals. In this realization, we have  $\tilde{D}_0 = 1$  and  $\tilde{D}_1 = \sin 2\theta$  irrespective of  $\alpha$ ,  $\tilde{C}_{00} = \tilde{C}_{01} = \frac{\alpha}{\sqrt{\sin^2 2\theta + \alpha^2}}$ ,  $\tilde{C}_{10} = -\tilde{C}_{11} = \frac{\sin 2\theta}{\sqrt{\sin^2 2\theta + \alpha^2}}$ , and Eq. (6) is saturated for a whole range of  $\alpha$  and  $\sin 2\theta$ .

It is known that any extremal nonclassical correlation in the simplest Bell scenario has a two-qubit realization, where projective measurements of rank 1 are performed on a pure entangled state [27]. For such extremal realizations, by applying appropriate local unitary transformations, Alice and Bob's observables are written as

$$A_x = \cos\theta_x^A \sigma_1 + \sin\theta_x^A \sigma_3, \quad B_y = \cos\theta_y^B \sigma_1 + \sin\theta_y^B \sigma_3, \quad (9)$$

where  $(\sigma_1, \sigma_3, \sigma_3)$  are the Pauli matrices. Moreover,  $\rho = |\psi\rangle\langle\psi|$  is chosen to be real symmetric, and let us express

$$\begin{aligned} \text{tr}_A(A_x \otimes I)|\psi\rangle\langle\psi| &= \alpha_x^B I + \beta_x^B (\cos\phi_x^B \sigma_1 + \sin\phi_x^B \sigma_3), \\ \text{tr}_B(I \otimes B_y)|\psi\rangle\langle\psi| &= \alpha_y^A I + \beta_y^A (\cos\phi_y^A \sigma_1 + \sin\phi_y^A \sigma_3) \end{aligned} \quad (10)$$

As shown in Appendix C, the necessary and sufficient condition for the saturation of Eq. (6) is given by

$$\sin(\phi_0^B - \theta_0^B) \sin(\phi_0^B - \theta_1^B) \sin(\phi_1^B - \theta_0^B) \sin(\phi_1^B - \theta_1^B) \leq 0. \quad (11)$$

Similarly, for the counterpart inequality on Alice's side,

$$\sin(\phi_0^A - \theta_0^A) \sin(\phi_0^A - \theta_1^A) \sin(\phi_1^A - \theta_0^A) \sin(\phi_1^A - \theta_1^A) \leq 0. \quad (12)$$

We have performed the Monte Carlo calculations, where a two-qubit realization to give the maximal violation of a randomly generated Bell expression is obtained. The numerical results suggest that Eq. (11) and (12) are simultaneously satisfied for all nonclassical extremal correlations, and hence support the following conjecture:

**Conjecture 1.** *For every extremal correlation, there always exists a realization such that the equality holds in Eq. (6) and in the counterpart inequality on Alice's side.*

In this way, most of correlations including the case of biased marginals appear to obey a simple and unified rule, which is revealed by considering the nonorthogonality between local states. Note that, when the real symmetric  $\rho$  is maximally entangled, Eq. (11) and (12), which specify a geometric relation between angles (see [26]), are necessary and sufficient for the extremality of the generated correlation with unbiased marginals. When the real symmetric  $\rho$  is chosen to be pure and partially entangled, do those provide a simple necessary and sufficient condition for the extremality also in the case of biased marginals? This is an intriguing open problem.

#### IV. INFORMATION THEORETICAL ASPECTS

To discuss the information theoretical aspects of the IC-type inequality Eq. (4), let us introduce a communication protocol. A nonlocal game known as the inner product game has been studied in connection to communication complexity [28, 29]. The protocol we consider is its communication version shown in Fig. 1, where Alice and Bob is given a random  $n$ -bit string  $\vec{x} = (x_1, \dots, x_n)$  and  $\vec{y} = (y_1, \dots, y_n)$  generated with the probability  $s_{\vec{x}}$  and  $t_{\vec{y}}$ , respectively. Alice (Bob) outputs a bit  $a_p$  ( $b_p$ ) utilizing shared quantum states, and she sends the message  $m$  to Bob that is  $a_p$  scrambled by an independent random bit  $r$  such as  $m = a_p \oplus r$ . The purpose of this protocol is that Bob obtains the value of  $(\vec{x} \cdot \vec{y}) \oplus r$ , where  $\vec{x} \cdot \vec{y} = \sum_i x_i y_i \bmod 2$ . The task is nontrivial even for  $\vec{y} = (0, \dots, 0)$  due to the scrambling by  $r$ . A more important role of  $r$  becomes clear later. Let  $A_{\vec{x}}$  ( $B_{\vec{y}}$ ) be the observable of Alice (Bob) to obtain  $a_p$  ( $b_p$ ), and the projector of Alice (Bob) be  $P_{a_p|\vec{x}}$  ( $Q_{b_p|\vec{y}}$ ). Then, Bob's success probability for a given  $\vec{y}$  averaged over  $\vec{x}$  is

$$\begin{aligned} p_{\vec{y}} &= \sum_{\vec{x}} s_{\vec{x}} \sum_{a_p b_p} \langle P_{a_p|\vec{x}} \otimes Q_{b_p|\vec{y}} \rangle \delta_{\vec{x} \cdot \vec{y} = a_p \oplus b_p} \\ &= \frac{1}{2} \left( 1 + \sum_{\vec{x}} s_{\vec{x}} \langle A_{\vec{x}} \otimes (-1)^{\vec{x} \cdot \vec{y}} B_{\vec{y}} \rangle \right). \end{aligned} \quad (13)$$

Concerning the quantum bound of the bias  $E_{\vec{y}} \equiv 2p_{\vec{y}} - 1$ , the discussion runs in parallel with Sec. II. Indeed,  $\sum_{\vec{x}} X_{\vec{x}}^2 = 2^n \sum_{\vec{y}} t_{\vec{y}}^2 I$  holds for  $X_{\vec{x}} \equiv \sum_{\vec{y}} t_{\vec{y}} (-1)^{\vec{x} \cdot \vec{y}} B_{\vec{y}}$ , hence  $\sum_{\vec{y}} t_{\vec{y}} E_{\vec{y}} \leq (2^n \sum_{\vec{x}} t_{\vec{y}}^2 s_{\vec{x}}^2 \tilde{D}_{\vec{x}}^2)^{\frac{1}{2}}$ , and we have  $\sum_{\vec{y}} E_{\vec{y}}^2 \leq 2^n \sum_{\vec{x}} s_{\vec{x}}^2 \tilde{D}_{\vec{x}}^2$ . Let us now assume that Alice and Bob utilize the  $n$  identical “quantum boxes”, each of which accepts inputs  $(x, y)$  and produces outputs  $(a, b)$  according to  $\{p(ab|xy)\}$ , and assume that  $a_p$  ( $b_p$ ) is the parity bit of Alice's (Bob's) outputs from the  $n$  boxes as shown in Fig. 1. Under those assumptions,  $B_{\vec{y}}$  must have a tensor product form such as  $B_{\vec{y}} = B_{y_1} \otimes B_{y_2} \otimes \dots$ , which implies that the maximization operator  $X$  in  $\tilde{D}_{\vec{x}}$  also has a tensor product form. It is then found that

$$\sum_{\vec{y}} E_{\vec{y}}^2 \leq \left( \frac{\tilde{D}_0^2 + \tilde{D}_1^2}{2} \right)^n \quad (14)$$

must hold in this protocol for  $s_{\vec{x}} = 1/2^n$ , whose right-hand side is the  $n$ -th power of the right-hand side of Eq. (4).

In the general setting of communication, where Alice is given  $\vec{x}$  and sends the bit string  $\vec{m}$  to Bob as a message, the information obtainable by Bob is characterized by the mutual information  $I(\vec{x} : \vec{m} \rho_B)$ , where  $\rho_B$  is the state of Bob's half of no-signaling resources. Using the no-signaling condition and the information-theoretical relations respected by quantum mechanics, it was shown that [8, 30, 31]

$$I(\vec{x} : \vec{m} \rho_B) = I(\vec{m} : \vec{x} \rho_B) - I(\vec{m} : \rho_B)$$

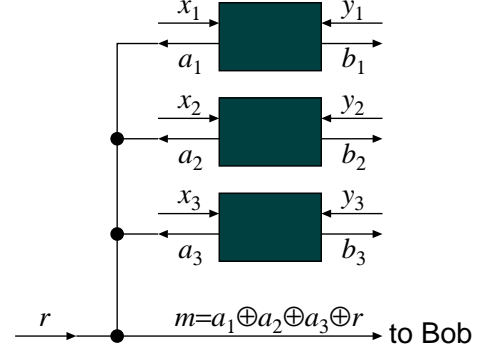


FIG. 1: The case of  $n=3$  is shown. The parity bit of all the outputs of the  $n$  boxes is scrambled by a random bit  $r$  and is sent to Bob as a message.

$$\leq H(\vec{m}) - H(\vec{m}|\vec{x} \rho_B) \leq H(\vec{m}). \quad (15)$$

Since the entropy  $H(\vec{m})$  cannot exceed the number of bits in  $\vec{m}$ , the IC principle is derived. The left-hand side of Eq. (14), where the  $2^n$  variables Bob tries to obtain are pair-wise independent [31–33], generally corresponds to the term  $I(\vec{x} : \vec{m} \rho_B)$ . To investigate the origin of the right-hand side of Eq. (14), let us focus on the term  $H(\vec{m}|\vec{x} \rho_B)$  omitted in the derivation of the IC principle (also in a generalization of the IC inequality [34]).

In the protocol of Fig. 1, since Alice is given  $\vec{x}$  and  $r$ , the relation corresponding to Eq. (15) is

$$I(\vec{x} r : m \rho_B) = H(m) - H(m|\vec{x} r \rho_B) = 1 - H(a_p|\vec{x} \rho_B), \quad (16)$$

where we took into account  $I(m : \rho_B) = 0$  and used  $H(m|\vec{x} r \rho_B) = H(a_p|\vec{x} \rho_B)$  because the conditional entropy  $H(X|Y) \equiv H(XY) - H(Y)$  means the remaining uncertainty of  $X$  after knowing  $Y$  (in the classical variable case). Let us then evaluate  $1 - H(a_p|\vec{x} \rho_B)$  in quantum mechanics. Considering the individual measurement strategy for boxes, the optimal success probability of guessing Alice's outcome  $a$  of a single box for the input  $x$  is given by  $(1 + \tilde{D}_x)/2$ , which is an operational meaning of the generalized trace distance. As shown in Appendix D, the result of the evaluation in the  $n \rightarrow \infty$  limit is then

$$1 - H(a_p|\vec{x} \rho_B) = \frac{1}{2 \ln 2} \left( \frac{\tilde{D}_0^2 + \tilde{D}_1^2}{2} \right)^n, \quad (17)$$

which appears to well correspond to the right-hand side of Eq. (14) (although there is a slight difference between  $\tilde{D}_x$  and  $\bar{D}_x$  in the case of mixed states).

In this way, it is found that the inequalities discussed in this paper represent the effects of the nonzero  $H(\vec{m}|\vec{x} \rho_B)$  in Eq. (15). For the nonzeroness, it is crucial whether or not Bob can completely determine Alice's outcome (abstractly denoted by  $\vec{a}$  hereafter) from the type of her measurement  $\vec{x}$  and his local state  $\rho_B$ . If he cannot do this, it implies  $H(\vec{a}|\vec{x} \rho_B) > 0$  and results in  $H(\vec{m}|\vec{x} \rho_B) > 0$  when  $\vec{m}$  is constructed from  $\vec{a}$  and  $\vec{x}$ . In this situation,  $\vec{a}$  appears to have some randomness and be scrambling

the information of  $\vec{x}$  encoded in  $\vec{m}$  from the viewpoint of Bob. This can occur not only when quantum resources are mixed states, but also pure states. Indeed, quantum correlations, which can be realized by partially entangled states (whose Schmidt coefficients are nondegenerate so that the Schmidt basis is unique), inevitably show  $H(\vec{a}|\vec{x}\rho_B) > 0$ , because Alice's measurements are non-commuting [35] and the basis of at least one measurement differs from the Schmidt basis. As a result, Bob's local states for different values of  $\vec{a}$  become nonorthogonal, and he cannot completely determine  $\vec{a}$ . It is a peculiar feature of quantum mechanics that there exist the extremal correlations that are realized by partially entangled states [13–16] and show  $H(\vec{a}|\vec{x}\rho_B) > 0$ , because every extremal correlation of both sets of classical and general no-signaling correlations (local deterministic correlations [5] and the Popescu-Rohrlich type boxes [3, 36]) does not show  $H(\vec{a}|\vec{x}\rho_B) > 0$ .

The randomness discussed above inevitably reduces the information obtainable by Bob. Indeed, it is clear from Eq. (15) that, for a quantum correlation that shows nonzero  $H(\vec{a}|\vec{x}\rho_B)$ , any protocol whose  $\vec{m}$  contains the information of  $\vec{a}$  and  $H(\vec{m}|\vec{x}\rho_B) > 0$  cannot achieve  $I(\vec{x} : \vec{m}\rho_B) = H(\vec{m})$  (the achievement is possible when  $\vec{m}$  does not contain the information of  $\vec{a}$ , but in that case the quantum correlation is not used by the protocol). This includes the case of the extremal correlations realized by partially entangled states discussed above. For those nonlocal correlations, the strength is constrained by a principle other than the IC principle. To investigate what the principle is, let us consider the protocol of Fig. 1 again. The point is that the message  $m$  is completely scrambled by  $r$ . As a result,  $I(\vec{x} : m\rho_B) = 0$  must hold by the cryptographic principle (or the principle of the information theoretic security), which states that a completely scrambled message (i.e., scrambled by independent random bits with the same number of the message bits) cannot carry information [19]. This cryptographic principle is derived in the same way as in [8] using the chain rule of mutual information  $[I(A : B|C) = I(A : BC) - I(A : C)]$  and the exchange symmetry  $[I(A : B|C) = I(B : A|C)]$  as

$$\begin{aligned} I(\vec{x} : m\rho_B) &= I(\vec{x} : \rho_B|m) + I(\vec{x} : m) \\ &= I(\rho_B : \vec{x}m) - I(\rho_B : m) = 0, \end{aligned} \quad (18)$$

where we used  $I(\vec{x}m : \rho_B) = 0$  by the no-signaling condition and used  $I(m : \vec{x}) = I(m : \rho_B) = 0$  by the independence of  $r$ . From this cryptographic principle, Eq. (16) is also obtained as

$$\begin{aligned} 0 &= I(\vec{x} : m\rho_B) = I(m\rho_B : \vec{x}r) - I(m\rho_B : r|\vec{x}) \\ &= I(\vec{x}r : m\rho_B) - I(r : \vec{x}m\rho_B) \\ &= I(\vec{x}r : m\rho_B) - I(m : \vec{x}r\rho_B) \\ &= I(\vec{x}r : m\rho_B) - 1 + H(a_p|\vec{x}\rho_B), \end{aligned} \quad (19)$$

where the independence of  $r$  was again used. From this, it is found that  $I(\vec{x}r : m\rho_B) > 1 - H(a_p|\vec{x}\rho_B)$  implies  $I(\vec{x} : m\rho_B) > 0$ ; the transmission of information of  $\vec{x}r$  be-

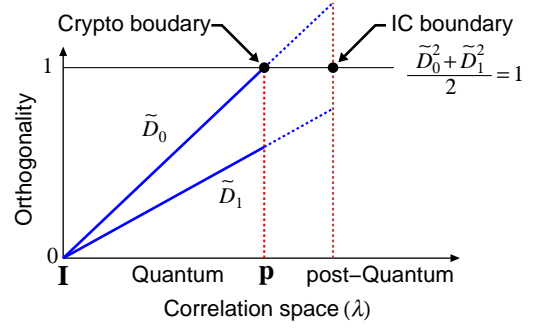


FIG. 2: The variation of  $\tilde{D}_0$  and  $\tilde{D}_1$  as a function of  $\lambda$  in the correlation space of  $\lambda\mathbf{p} + (1-\lambda)\mathbf{I}$ , where  $\mathbf{p}$  is a boundary correlation.

yond  $1 - H(a_p|\vec{x}\rho_B)$  implies that the completely scrambled message  $m$  would carry information of  $\vec{x}$ . Namely, the strength of the nonlocal correlation is constrained so that the violation of the cryptographic principle does not occur. The inequalities derived in this paper represent the effects of nonzero  $H(a_p|\vec{x}\rho_B)$ , and those can be said to be cryptographic quantum bounds on nonlocality.

## V. BOUNDARY CONDITION

The information theoretical relation representing the cryptographic principle is an equality such as Eq. (19), which is consistent with the fact that the equality of Eq. (6) widely holds not only for boundary correlations but also for non-boundary correlations. However, this is an undesirable property for the purpose of identifying the quantum boundaries. Nevertheless, the cryptographic bounds tell us a way to determine the boundaries. The two-qubit realization shown in [14] and discussed in Sec. III again gives an informative example. Consider the boundary correlation that maximally violates the Bell expression  $\frac{2}{\sqrt{3}}\langle A_0 \rangle + \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$ , where  $|\psi\rangle = \sqrt{2/3}|00\rangle + \sqrt{1/3}|11\rangle$ ,  $\langle A_0 \rangle = 1/3$ ,  $\langle A_1 \rangle = 0$ ,  $\langle B_0 \rangle = \langle B_1 \rangle = 1/\sqrt{17}$ ,  $\langle A_0 B_0 \rangle = \langle A_0 B_1 \rangle = 3/\sqrt{17}$ ,  $\langle A_1 B_0 \rangle = -\langle A_1 B_1 \rangle = 8/\sqrt{17}/3$ ,  $\tilde{D}_0 = 1$ , and  $\tilde{D}_1 = \sqrt{8}/3$ . This is the same as the simple example shown in Sec. I. For this boundary correlation, the IC inequality is not saturated as  $E_0^2 + E_1^2 = 17/18 < 1$ , while the cryptographic bound of the IC-type Eq. (4) is saturated as  $(\tilde{D}_0^2 + \tilde{D}_1^2)/2 = 17/18$ . Note that, since the left-hand side is the same for both inequalities, the saturation of the IC-type inequality implies that the protocol used for the derivation of the IC inequality in [8] is already optimal for maximizing the left-hand side.

Let us then consider the correlation of the form Eq. (7) with  $\mathbf{p}$  being the boundary correlation. As discussed in Sec. III,  $\tilde{D}_0$  and  $\tilde{D}_1$  of  $\mathbf{q}$  that saturate Eq. (6) vary linearly with  $\lambda$  as schematically shown in Fig. 2. It is then found that the quantum boundary is determined such that  $\tilde{D}_0$  reaches the maximum limit of 1. Indeed, if  $\tilde{D}_0$

only takes 1 over all possible realizations of a correlation, the correlation must be located at a boundary, because, if  $\mathbf{q}$  with  $\lambda = \lambda_0 > 1$  is quantum realizable,  $\mathbf{p}$  has a realization with  $\tilde{D}_0 = 1/\lambda_0 < 1$ , which causes a contradiction. This is indeed the case of  $\mathbf{p}$  because the realization was shown to be unique up to local unitary transformations [14].

In this way,  $\tilde{D}_0$  and  $\tilde{D}_1$ , which must not exceed 1, individually set a limit to determine the quantum boundaries. Every boundary in the case of unbiased marginals can be identified in such a way by Lemma 1. This is the case of local deterministic correlations also, where either  $\text{tr}\rho_{0|x} = 0$  or  $\text{tr}\rho_{1|x} = 0$  holds and there is no realization with  $\tilde{D}_x < 1$ . Unfortunately, however, the results of the Monte Carlo calculations indicate that both  $\tilde{D}_0$  and  $\tilde{D}_1$  (and Alice's counterparts) are generally less than 1 for extremal correlations with biased marginals, i.e., most are determined by another limit, in spite that the equality of Eq. (6) is respected. What is the principle to fully identify the boundaries? This still remains open.

## VI. SUMMARY

To conclude, we obtained the nonlocality inequalities in the simplest Bell scenario, which must be respected by quantum mechanics and include the effects of the randomness produced in the message when quantum resources such as partially entangled states and mixed states are used for communication. The randomness originates from the nonorthogonality of receiver's states and the effects enter the inequalities through the trace distancelike quantity, which is hence close to the bias of the optimal success probability of guessing the sender's measurement outcome, when assuming that a receiver knows the type of the measurement. The obtained inequalities reflect the constraint by the cryptographic principle. This is due to the fact that the randomness reduces the information obtainable by a receiver, and the transmission of information beyond the reduction implies that a completely scrambled message would carry information.

Introducing the cryptographic principle to nonlocality inequalities leads to two effects. First, the inequalities come to be saturated inside the set of quantum correlations. Indeed, the obtained Landau-type inequality is saturated for all (boundary and non-boundary) correlations with unbiased marginals. We conjecture that the inequality is saturated for every extremal correlation even with biased marginals, i.e., most of nonlocal correlations in the simplest Bell scenario obey a simple and unified rule. Second, the maximum limit of one message bit set by the information causality principle splits into the two trace distancelike quantities, which must not exceed 1 and individually set a limit to determine the quantum boundaries. Namely, the maximality of the orthogonality (or vanishment of the above mentioned randomness) play an important role in determining some of the quantum boundaries.

## Acknowledgments

This work was supported by JSPS KAKENHI Grant No. 24540405.

## Appendix A: Properties of $\tilde{D}$

Some properties of the trace distancelike quantity

$$\tilde{D}(\rho, \sigma) = \max_X \frac{\text{tr}X(\rho - \sigma)}{\sqrt{\text{tr}X^2(\rho + \sigma)}}, \quad (\text{A1})$$

between subnormalized  $\rho$  and  $\sigma$  are proved here. Without loss of generality, we can assume  $\text{tr}(\rho + \sigma) = 1$ , otherwise renormalize  $\rho$  and  $\sigma$ . Since the maximization is taken over all Hermitian operators  $X$ , the constraint of  $\text{tr}X^2(\rho + \sigma) = 1$  does not alter the optimization result, and hence let us maximize

$$\text{tr}X(\rho - \sigma) - l(\text{tr}X^2(\rho + \sigma) - 1), \quad (\text{A2})$$

where  $l$  is the Lagrange multiplier. The extremal condition with respect to the small deviation of  $X \rightarrow X + \Delta X$ , where  $\Delta X$  is any Hermitian operator, is given by

$$Y \equiv \rho - \sigma - l(\rho + \sigma)X - lX(\rho + \sigma) = 0. \quad (\text{A3})$$

In the case of pure states, let  $\rho = p|0\rangle\langle 0|$  and  $\sigma = (1 - p)|\phi\rangle\langle\phi|$  where  $|\phi\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle$ , and let  $X = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ . From  $\langle 1|Y|1\rangle = 0$  and  $\langle \phi_\perp|Y|\phi_\perp\rangle = 0$ , where  $|\phi_\perp\rangle = \sin\phi|0\rangle - \cos\phi|1\rangle$ , we have  $a + c = 0$  and hence  $X^2 = (a^2 + b^2)I = I$  so that  $\text{tr}X^2(\rho + \sigma) = 1$ . Since

$$\bar{D}(\rho, \sigma) \equiv \text{tr}|\rho - \sigma| = \max_{X^2=I} \text{tr}X(\rho - \sigma), \quad (\text{A4})$$

we have  $\tilde{D}(\rho, \sigma) = \bar{D}(\rho, \sigma)$  in the case of pure states. In the other general cases,  $\tilde{D}(\rho, \sigma) \geq \bar{D}(\rho, \sigma)$  is obvious.

Moreover, let  $\rho - \sigma = Q - S$  where  $Q$  and  $S$  are positive operators with orthogonal support. Since  $|\rho - \sigma| \leq \rho + \sigma$ ,  $\text{tr}(Q + S) = \text{tr}|\rho - \sigma|$ , and  $\tilde{D}(\rho, \sigma) = 1$  if  $\rho$  and  $\sigma$  are orthogonal, we have

$$\begin{aligned} \tilde{D}(\rho, \sigma) &\leq \max_X \frac{\text{tr}X(\rho - \sigma)}{\sqrt{\text{tr}X^2|\rho - \sigma|}} = \max_X \frac{\text{tr}X(Q - S)}{\sqrt{\text{tr}X^2(Q + S)}} \\ &= \sqrt{\text{tr}(Q + S)} = \sqrt{\bar{D}(\rho, \sigma)}. \end{aligned} \quad (\text{A5})$$

Therefore,  $\bar{D}(\rho, \sigma) \leq \tilde{D}(\rho, \sigma) \leq \sqrt{\bar{D}(\rho, \sigma)}$ , and hence  $\tilde{D}(\rho, \sigma) = 1$  if and only if  $\bar{D}(\rho, \sigma) = 1$ .

The optimization with respect to  $X$  in Eq. (A1) can be performed analytically as follows. Let  $|i\rangle$  be the eigenstate of  $\rho + \sigma$ , i.e.,  $(\rho + \sigma)|i\rangle = \lambda_i|i\rangle$ , and  $x_{ij} \equiv \langle i|X|j\rangle$ . We then have

$$\text{tr}X^2(\rho + \sigma) = \sum_i \lambda_i (x_{ii})^2 + \sum_{j>i} (\lambda_i + \lambda_j) |x_{ij}|^2$$

$$= \sum_i (x'_{ii})^2 + \sum_{j>i} |x'_{ij}|^2 = 1, \quad (\text{A6})$$

where  $x'_{ii} \equiv \sqrt{\lambda_i} x_{ii}$  and  $x'_{ij} \equiv \sqrt{\lambda_i + \lambda_j} x_{ij}$  for  $i \neq j$ . Moreover, using  $a_{ij} = \langle i | \rho - \sigma | j \rangle$ , we have

$$\begin{aligned} \text{tr} X(\rho - \sigma) &= \sum_i x_{ii} a_{ii} + \sum_{j>i} (x_{ij} a_{ij}^* + x_{ij}^* a_{ij}) \\ &= \sum_i \frac{x'_{ii} a_{ii}}{\sqrt{\lambda_i}} + \sum_{j>i} \frac{x'_{ij} a_{ij}^* + x_{ij}^* a_{ij}}{\sqrt{\lambda_i + \lambda_j}}. \end{aligned} \quad (\text{A7})$$

Since  $\tilde{D}(\rho, \sigma)$  is given by the maximum of Eq. (A7) under the constraint of Eq. (A6), we have

$$\tilde{D}(\rho, \sigma) = \left( \sum_i \frac{(a_{ii})^2}{\lambda_i} + \sum_{j>i} \frac{4|a_{ij}|^2}{\lambda_i + \lambda_j} \right)^{\frac{1}{2}} = \left( \sum_{ij} \frac{2|a_{ij}|^2}{\lambda_i + \lambda_j} \right)^{\frac{1}{2}}.$$

### Appendix B: Landau-type inequality

In the CHSH expression with general weight parameters, if we define  $X_x = u_{x0} B_0 + (-1)^x u_{x1} B_1$ , we have  $X_0^2 + X_1^2 = \sum_{xy} u_{xy}^2 I$  by virtue of  $u_{00} u_{01} = u_{10} u_{11}$ , and hence obtain Eq. (5). When  $\tilde{D}_0, \tilde{D}_1 > 0$ , we have

$$\sum_x (u_{x0} \tilde{C}_{x0} + (-1)^x u_{x1} \tilde{C}_{x1})^2 \leq \sum_{xy} u_{xy}^2. \quad (\text{B1})$$

Noticing  $\tilde{C}_{xy}^2 \leq 1$  and using  $v_{xy} \equiv u_{xy}(1 - \tilde{C}_{xy}^2)^{\frac{1}{2}}$ , this is rewritten as

$$(\tilde{C}_{00} \tilde{C}_{01} - \tilde{C}_{10} \tilde{C}_{11}) v_{00} v_{01} \leq (1 - \tilde{C}_{00}^2)^{\frac{1}{2}} (1 - \tilde{C}_{01}^2)^{\frac{1}{2}} \sum_{xy} \frac{1}{2} v_{xy}^2.$$

Since  $u_{00} u_{01} = u_{10} u_{11}$ , it can be seen that

$$\begin{aligned} &(1 - \tilde{C}_{00}^2)^{\frac{1}{2}} (1 - \tilde{C}_{01}^2)^{\frac{1}{2}} \sum_{xy} \frac{1}{2} v_{xy}^2 \\ &\geq (1 - \tilde{C}_{00}^2)^{\frac{1}{2}} (1 - \tilde{C}_{01}^2)^{\frac{1}{2}} (|v_{00} v_{01}| + |v_{10} v_{11}|) \\ &= [(1 - \tilde{C}_{00}^2)^{\frac{1}{2}} (1 - \tilde{C}_{01}^2)^{\frac{1}{2}} + (1 - \tilde{C}_{10}^2)^{\frac{1}{2}} (1 - \tilde{C}_{11}^2)^{\frac{1}{2}}] |v_{00} v_{01}|, \end{aligned}$$

and we obtain Eq. (6). In the case of  $\tilde{D}_{x0} = 0$  for either  $x_0 = 0$  or 1,  $C_{x0y} = 0$  holds because  $\tilde{D}_{x0} \geq |C_{x0y}|$  by definition, and we have Eq. (6) in which  $\tilde{C}_{x00} = \tilde{C}_{x01} = 0$ .

Similarly, for a tilted CHSH expression, we have

$$\begin{aligned} &\sum_{xy} s_x u_{xy} (-1)^{xy} \langle (A_x + \epsilon_x I) \otimes B_y \rangle \\ &\leq \left[ \sum_{xy} u_{xy}^2 \right]^{\frac{1}{2}} \left[ \sum_x s_x^2 (\tilde{D}_x^\epsilon)^2 \right]^{\frac{1}{2}}, \end{aligned} \quad (\text{B2})$$

where  $u_{00} u_{01} = u_{10} u_{11}$  again,  $\epsilon_x$  is real, and

$$\tilde{D}_x^\epsilon \equiv \max_X \frac{\text{tr} X[(1 + \epsilon_x) \rho_{0|x} - (1 - \epsilon_x) \rho_{1|x}]}{\sqrt{\text{tr} X^2(\rho_{0|x} + \rho_{1|x})}}. \quad (\text{B3})$$

In the same way as Appendix A, it is not difficult to see  $(\tilde{D}_x^\epsilon)^2 = \tilde{D}_x^2 + 2\epsilon_x \langle A_x \rangle + \epsilon_x^2$ . When  $\tilde{D}_0^2 > \langle A_0 \rangle^2$  and

$\tilde{D}_1^2 > \langle A_1 \rangle^2$ , the necessary and sufficient condition of Eq. (B2) is again Eq. (6) but with

$$\tilde{C}_{xy} \equiv \frac{C_{xy} - \langle A_x \rangle \langle B_y \rangle}{(\tilde{D}_x^2 - \langle A_x \rangle^2)^{\frac{1}{2}} (1 - \langle B_y \rangle^2)^{\frac{1}{2}}}. \quad (\text{B4})$$

This is an extension of the NPA inequality [24, 25].

### Appendix C: Extremal correlation

Under the parametrization of Eq. (9), the expectation of the Bell expression  $\sum_{abxy} V_{abxy} p(ab|xy)$  with  $p(ab|xy) = \langle \psi | P_{a|x} \otimes Q_{b|y} | \psi \rangle$  is maximized when  $\rho = |\psi\rangle\langle\psi|$  is real symmetric. A necessary and sufficient condition for the saturation of Eq. (6) is that it is possible to assign nontrivial values to  $u_{xy}$  such that Eq. (5) is saturated (and  $u_{00} u_{01} = u_{10} u_{11}$ ). This is possible only when  $X_x = \sum_y (-1)^{xy} u_{xy} B_y$  agrees with the operator of maximizing  $\tilde{D}_x$ . Note that  $\rho$  is pure and the projector is rank 1,  $\rho_{a|x}$  is also pure and  $\tilde{D}_x = \bar{D}_x$ . Since the operator of maximizing  $\tilde{D}_x$  is then unique up to the normalization, we have  $X_x \propto \cos \phi_x^B \sigma_1 + \sin \phi_x^B \sigma_3$  hence  $\sum_y (-1)^{xy} u_{xy} \sin(\phi_x^B - \theta_y^B) = 0$ . In order that  $u_{00} u_{01} = u_{10} u_{11}$ ,  $-\sin(\phi_1^B - \theta_0^B) \sin(\phi_0^B - \theta_1^B) u_{00}^2 = \sin(\phi_0^B - \theta_1^B) \sin(\phi_1^B - \theta_0^B) u_{11}^2$  and  $-\sin(\phi_0^B - \theta_1^B) \sin(\phi_1^B - \theta_0^B) u_{01}^2 = \sin(\phi_1^B - \theta_0^B) \sin(\phi_0^B - \theta_1^B) u_{10}^2$  must hold, and we obtain Eq. (11). Since there are no other constraints for  $u_{xy}$ , we can assign nontrivial values to  $u_{xy}$  if Eq. (11) is satisfied.

### Appendix D: Evaluation of $1 - H(a_p | \vec{x} \rho_B)$

Let us denote Bob's guess for the parity bit  $a_p$  (for a given  $\vec{x}$ ) under the individual measurement strategy for boxes by  $b_p$ , the conditional probability by  $P_{a_p|b_p}$ , and the other probabilities similarly. Let us then evaluate the leading term of  $H(a_p | b_p)$  given by

$$\begin{aligned} H(a_p | b_p) &= P_{b_p=0} h(P_{0|0}) + P_{b_p=1} h(P_{1|1}) \\ &\approx 1 - \frac{1}{2 \ln 2} [P_{b_p=0} (2P_{0|0} - 1)^2 + P_{b_p=1} (2P_{1|1} - 1)^2] \\ &= 1 - \frac{1}{2 \ln 2} \left[ \frac{(P_{a_p=b_p} - P_{a_p=1})^2}{P_{b_p=0}} + \frac{(P_{a_p=b_p} - P_{a_p=0})^2}{P_{b_p=1}} \right], \end{aligned}$$

for  $k \gg 1$  and  $n - k \gg 1$  with  $k$  being the number of 0 in a given  $\vec{x}$  (see also [37]). Since the optimal success probability of guessing  $a$  for a single box is  $(1 + \bar{D}_x)/2$ , the optimal probability for  $a_p$  is given by  $P_{a_p=b_p} = (1 + \bar{D}_0^k \bar{D}_1^{n-k})/2$ . Using Alice's marginals  $p(a|x)$  of a single box, we have

$$P_{a_p=0} = \frac{1}{2} [1 + (2p(0|0) - 1)^k (2p(0|1) - 1)^{n-k}]. \quad (\text{D1})$$

Suppose that  $\rho_{0|x}$  and  $\rho_{1|x}$  are nonorthogonal. Moreover,  $\text{sup}(\rho_{0|x})$  and  $\text{sup}(\rho_{1|x})$  are not identical in general. This implies  $|2p(0|x) - 1| < \bar{D}_x < 1$ , and hence the leading

term comes from  $\bar{D}_0^k \bar{D}_1^{n-k}$ . As a result, since  $H(a_p|b_p) \approx 1 - \bar{D}_0^{2k} \bar{D}_1^{2(n-k)} / (2 \ln 2)$ , we have

$$1 - H(a_p|\vec{x}\rho_B) = 1 - \frac{1}{2^n} \sum_{\vec{x}} H(a_p|b_p)$$

$$\approx \frac{1}{2 \ln 2} \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} \bar{D}_0^{2k} \bar{D}_1^{2(n-k)} = \frac{1}{2 \ln 2} \left( \frac{\bar{D}_0^2 + \bar{D}_1^2}{2} \right)^n.$$

- 
- [1] J. Bell, *Physics* **1**, 195 (1964).
  - [2] B. S. Cirel'son, *Lett. Math. Phys.* **4**, 93 (1980).
  - [3] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
  - [4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
  - [5] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Rev. Mod. Phys.* **86**, 419 (2014).
  - [6] S. Popescu, *Nat. Phys.* **10**, 264 (2014).
  - [7] G. Oas and J. A. de Barros, *Contextuality from Quantum Physics to Psychology* (World Scientific, Singapore, 2016), chap. 15, pp. 335–366.
  - [8] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, *Nature (London)* **461**, 1101 (2009).
  - [9] J. Allcock, N. Brunner, M. Pawłowski, and V. Scarani, *Phys. Rev. A* **80**, 040103 (2009).
  - [10] B. S. Tsirelson, *J. Sov. Math.* **36**, 557 (1987).
  - [11] L. J. Landau, *Found. Phys.* **18**, 449 (1988).
  - [12] L. Masanes, arXiv:quant-ph/0309137.
  - [13] Y.-C. Liang, T. Vértesi, and N. Brunner, *Phys. Rev. A* **83**, 022108 (2011).
  - [14] A. Acín, S. Massar, and S. Pironio, *Phys. Rev. Lett.* **108**, 100402 (2012).
  - [15] R. Ramanathan, D. Goyeneche, P. Mironowicz, and P. Horodecki, arXiv:1506.05100.
  - [16] Y.-Z. Zhen, K. T. Goh, Y.-L. Zheng, W.-F. Cao, X. Wu, K. Chen, and V. Scarani, *Phys. Rev. A* **94**, 022116 (2016).
  - [17] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, *Phys. Rev. Lett.* **107**, 210403 (2011).
  - [18] T. H. Yang, D. Cavalcanti, M. L. Almeida, C. Teo, and V. Scarani, *New J. Phys.* **14**, 013061 (2012).
  - [19] C. E. Shannon, *Bell System Technical Journal* **28**, 656 (1949).
  - [20] A. Y. Carmi and D. Moskovich, arXiv:1507.07514.
  - [21] T. Lowson, N. Linden, and S. Popescu, arXiv:1011.6245 (2010).
  - [22] T. Vértesi and K. F. Pál, *Phys. Rev. A* **77**, 042106 (2008).
  - [23] Y.-C. Liang and A. C. Doherty, *Phys. Rev. A* **75**, 042103 (2007).
  - [24] M. Navascués, S. Pironio, and A. Acín, *Phys. Rev. Lett.* **98**, 010401 (2007).
  - [25] M. Navascués, S. Pironio, and A. Acín, *New J. Phys.* **10**, 073013 (2008).
  - [26] Y. Wang, X. Wu, and V. Scarani, *New J. Phys.* **18**, 025021 (2016).
  - [27] L. Masanes, *Phys. Rev. Lett.* **97**, 050503 (2006).
  - [28] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Rev. Mod. Phys.* **82**, 665 (2010).
  - [29] W. van Dam, *Natural Computing* **12**, 9 (2013).
  - [30] O. C. O. Dahlsten, D. Lercher, and R. Renner, *New J. Phys.* **14**, 063024 (2012).
  - [31] S. W. Al-Safi and A. J. Short, *Phys. Rev. A* **84**, 042323 (2011).
  - [32] M. Pawłowski and A. Winter, *Phys. Rev. A* **85**, 022331 (2012).
  - [33] M. Bavarian and P. W. Shor, *Proc. of 2015 Conference on Innovations in Theoretical Computer Science (ITCS '15)* p. 123 (2015).
  - [34] R. Chaves, C. Majenz, and D. Gross, *Nat. Commun.* **6**, 5766 (2014).
  - [35] A. Fine, *Phys. Rev. Lett.* **48**, 291 (1982).
  - [36] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, *Phys. Rev. A* **71**, 022101 (2005).
  - [37] C. H. Bennett, T. Mor, and J. A. Smolin, *Phys. Rev. A* **54**, 2675 (1996).